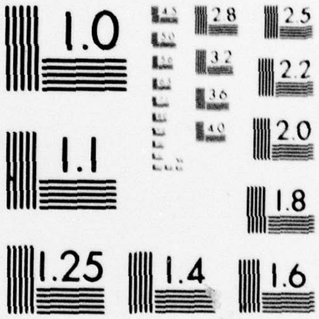
AD-A071 745 UNIVERSITY OF SOUTHERN CALIFORNIA LOS ANGELES DEPT O--ETC F/G 9/4
RESEARCH IN COMMUNICATION THEORY.(U)
JUN 79 R A SCHOLTZ, L R WELCH DAAG29-76-G-0246

UNCLASSIFIED ARO-13728.9-EL NL

| OF |

AD
A071745

END
DATE
FILMED
8-79
DDC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER (1) 13728.9-EL (18) ARO	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) RESEARCH IN COMMUNICATION THEORY. (6) (11)		5. TYPE OF REPORT & PERIOD COVERED (9) Final Report, 16 Jun 76 - 15 Jun 79
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) R. A. Scholtz L. R. Welch (10)		8. CONTRACT OR GRANT NUMBER(s) (15) DAAG29-76-G-0246
9. PERFORMING ORGANIZATION NAME AND ADDRESS University of Southern California Electrical Engineering Department Los Angeles, California 90007		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P. O. Box 12211 Research Triangle Park, NC 27709		12. REPORT DATE (11) Jun 79
		13. NUMBER OF PAGES 7
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) (12) 9 P'		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

LEVEL

16. DISTRIBUTION STATEMENT (of this Report)

A071745

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

The view, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

spread spectrum concept
bent-function sequences
burst-error channels
decoding
coding
decoders
communication theory

20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The major results of research performed on this grant have been published or are pending publication. This report contains the following abstracts which indicates the breadth and depth of results: The Spread Spectrum Concept; Group Characters: Sequences with Good Correlation Properties; Bent-Function Sequences; A Class of Binary Balanced Sequences; Partial-Period Correlation Properties of PN Sequences; Spectral Shaping Without Subcarriers; Continued Fractions and Berlekamp's Algorithm; The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions; Recursive Decoders for Convolutional Codes Transmitted Over Burst Channels; and Mutual Decoding and Generalized Code Interleaving in Burst-Error Channels. (9)

FINAL REPORT

"Research in Communication Theory"
Army Research Office Grant DAAG29-76-G-0246
with

R.A. Scholtz and L.R. Welch
Electrical Engineering Department
University of Southern California
Los Angeles, CA 90007

RESEARCH IN COMMUNICATION THEORY

A Summary of Results

Most of the major results of research performed on this grant have been published or are pending publication. Here is a listing of abstracts which indicates the breadth and depth of results.

The Spread Spectrum Concept

This paper describes an idealized spread-spectrum communication system. The processing gain concept is developed as a measure of a well-designed system's robust performance against independent wide-sense stationary interference. Multipath and repeater jammer rejection, partial correlation problems and security requirements are related to spread-spectrum code properties.

Group Characters: Sequences with Good Correlation Properties

The structure of the group of integers relatively prime to n under multiplication modulo n is reviewed, and the basic properties of characters defined on that group is developed. Appropriately chosen subcollections of the characters when viewed as periodic sequences are then shown to have relatively ideal auto-correlation and cross-correlation properties, making them suitable for spread-spectrum CDMA signalling. The results of a computer study indicate that the same subcollections when viewed as finite length sequences also have very good aperiodic autocorrelation and cross correlation properties.

Bent-Function Sequences

A class of nonlinear binary sequences is developed which asymptotically achieve Welch's lower bound on simultaneous cross-correlation and auto-correlation magnitudes. The sequences are constructed by applying nonlinear feed-forward functions on an n stage maximum-length linear-feedback shift-register generator in the Galois configuration. This technique has an additional attribute for many applications because the resulting sequences are nonlinear in that the order of the linear difference equation satisfied by the sequence can be orders of magnitude larger than the number of memory elements in the generator. A class of optimum codes is obtained when $n=0$ (mod 4) and are called affine-subspace bent-function sequences. The period of the codes is 2^n-1, they are balanced and have three valued cross-correlation functions and three valued out-of-phase autocorrelation. The correlation magnitudes are $\leq 2^{n/2}+1$,

$\sqrt{2}$ better than Gold Codes. The hardware complexity of these nonlinear generators is approximately the same as that of a Gold Code Generator. The size of the class is $2^{n/2}$.

A Class of Binary Balanced Sequences

This dissertation covers a class of binary sequences (± 1) with good correlation properties. Such sequences are known to play a significant role in many communication problems.

In a wide variety of situations arising in electronics, in digital computer work, in radar, in spread spectrum, in cryptography, in ranging systems and in numerous other fields, a need arises for sequences with small correlation.

The class of binary sequences studied in this dissertation is defined by the following requirements: (a) The length of the sequence is a power of 2. (b) The number of +1's equals the number of -1's; sequences satisfying this condition are referred to as balanced. (c) The cyclic correlation function out-of-phase has only three values: -4,0,+4. Sequences that satisfy requirements a, b and c will be defined as good balanced sequences. The goal of this research was to find good balanced sequences of different lengths and explore methods of generating them. Intuitively, it seemed that there would not be many solutions to this problem.

In order to find the good balanced sequences of lengths, 4,8 and 16 exhaustive computer search can be employed successfully in reasonable short machine time. Simple exhaustion at levels 32 and 64 was prohibitively expensive in terms of machine time; it was necessary to develop strategies that allowed the problem to be handled within practical computation limits.

Efficiency of search can be increased substantially by introducing the use of a group of symmetries. The symmetry group generated by cyclic shifting, decimation and complementation can be used to considerable shorten the search procedure.

A different strategy applied to lenghth 64, based on a tree search, is developed. While the strategy is quite efficient, the number of surviving branches at the fifth level indicated that the full search would be prohibitvely expensive in terms of computer time. The search was modified by randomly sampling the tree structure to obtain estimates of running time for a complete search. In the process of this study one good balanced sequence of length 64 was found.

Partial-Period Correlation Properties of PN Sequences

This paper outlines a systematic procedure for obtaining bounds on the distribution F(z) of partial-period correlation values of sets of periodic sequences. The ability to carry out the procedure depends on the development of linear code ß from the sequence set. Using the MacWilliams-Pless identities, moments of F(z) can be related to the weight distribution of the dual code $\beta^{\perp}$. Bounds on F(z) are then calculated using the theory developed to solve the classical moment problem.

Spectral Shaping Without Subcarriers

For proper operation of the phase lock loop which tracks a carrier it is important to minimize the spectral energy at frequencies near the carrier. A traditional method is to modulate the data onto a subcarrier in such a way that there is little energy near D.C. The resulting signal then is used to modulate the carrier. The problem with such a scheme is that the total bandwidth is much larger than necessary to transmit the data. This paper proposes and analyzes a simpler scheme which increases the data bandwidth by a very small fraction, yet reduces the energy near D.C. to nearly zero.

Continued Fractions and Berlekamp's Algorithm

Theorems are presented concerning the optimality of rational approximations using non-Archimedean norms. The algorithm for developing the rational approximations is based on continued fraction techniques and is virtually equivalent to an algorithm employed by Berlekamp for decoding BCH codes. Several variations of the continued fraction technique and Berlekamp's algorithm are illustrated on a common example.

The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions

It is shown that Reed-Solomon (RS) codes can be decoded by using a fast Fourier transform (FFT) algorithm over finite fields GF(F_n), where F_n is a Fermat prime, and continued fractions. This new transform decoding method is simpler than the standard method for RS codes. The computing time of this new decoding algorithm in software can be faster than the standard decoding method for RS codes.

Recursive Decoders for Convolutional Codes Transmitted Over Burst Channels

Convolutional codes have been used against burst channels, but the main emphasis in this area has been placed on devising special codes which are threshold decodable and on standard interleaving of random error correcting codes.

This work addresses the problem of using Viterbi type decoders in the decoding of convolutional codes transmitted over finite state channels.

A modified Viterbi algorithm which minimizes the probability of error in jointly estimating the sequences of encoder and channel states is presented. Digital computer simulation was used to compare the performance of the algorithm against a two-state burst-channel with that of standard Viterbi decoder. An upper bound to the performance of the modified decoder is developed by use of flow graph techniques. A lower bound to the performance is obtained using a genie argument.

The same genie concept is used to develop a class of adaptive decoders which have complexity growth with the number of channel states smaller than the modified decoder. These decoders therefore are useful whenever the channel model contains several states.

Standard decoding procedures for interleaved codes are not efficient, since no information concerning the channel state is passed along from decoder to decoder. A more efficient class of (adaptive) interleaved decoders is obtained by using the genie concept. If enough delay is allowed, these decoders represent a promising way of approaching in practice the performance of the (ideal) genie decoder.

Mutual Decoding and Generalized Code Interleaving in Burst-Error Channels

This thesis deals with the problem of communicating in burst-error channels. Burst-error channels are used to represent a large class of modern communication media; and the problem of communicating reliably through such media has received much study. Existing techniques include two-way communication scheme that involve error-detection and retransmission, and one-way scheme that utilizes error correcting codes in code interleaving. The error-detection and retransmission scheme is simple but its applicability is restricted to limited environments. On the other hand, the concept of code interleaving has proved to be a very versatile and effective technique for dealing with burst-error channels. In the code interleaving scheme, code symbols from a number of component codes are interleaved before being sent through the channel. This method effectively distributes the error-detection and correction burden amongst the component codes and thus lowers the overall redundancy requirement. However, the memory characteristics of the burst-error channel have not been used. This prompts the investigation presented in this thesis to take advantage of such inherent information embedded in the code interleaving scheme when used with burst-error channels. Two ideas to accomplish this goal are explored namely, mutual decoding and generalized code interleaving.

Mutual decoding is aimed at utilizing information obtained in decoding the first component code to aid in locating errors for the second component code. It is found that the average burst length of the channel, the depth of interleaving, the symbol depths and the work lengths of the component codes are determining parameters contributing to improved performance of the channel. The proper relationships between these parameters also suggest some useful coding and decoding strategies.

In the generalized code interleaving scheme, attempts are made to alter error characteristics of the channel by incorporating matched pre- and post-processing of the channel bit sequence. By re-distributing the error locations, it was hoped that the first component code can be designed to be principally an error-correcting code with the subsequent codes basically erasure codes. Unfortunately, this method is found to be ineffective for the class of code-channel combinations under investigation.

Performance criteria are set up to facilitate performance evaluation. Theoretical formulations are also devised to predict code performance and their validity is verified using computer simulations. Performance is also compared with the theoretically achievable capacities of the channels involved.

CONTINUING EFFORTS

During the last six months of the grant we have been working in three problem areas: (a) the enlargement and generalization of sequence sets developed from bent functions; (b) coding for spectral shaping; and (c) the construction of completely coherent wideband multiple frequency systems. Portions of the work will be continued under Grant No. DAAG29-79-C-0054.

Personnel Supported 6/16/76 through 6/15/79:

R.A. Scholtz (Principal Investigator)
L.R. Welch (Principal Investigator)
J. Libman (Research Assistant, Ph.D. received June 1977)
J.R. de Marca (Research Assistant, Ph.D. received June 1977)
N.E. Bekir (Research Assistant, Ph.D. received Jan. 1978)
K. Leung (Research Assistant, Ph.D. received June 1978)
J.D. Olsen (Research Assistant, Ph.D. received Jan. 1978)
D. McCollom (Research Assistant)
J.S. Soh (Research Assistant)

Theses Published:

1. J. Libman, "A Class of Binary Balanced Sequences," June 1977.

2. J.R.B. deMarca, "Recursive Decoders for Convolutional Codes Transmitted Over Burst Channels," June 1977.

3. N.E. Bekir, "Bounds on the Distribution of Partial Correlation for PN and Gold Sequences", January 1978.

4. K.S. Leung, "Mutual Decoding and Generalized Code Interleaving in Burst-Error Channels", June 1978.

5. J.D. Olsen, "Nonlinear Binary Sequences with Asymptotically Optimum Periodic Cross-Correlation", December 1977.

Papers Published:

1. R.A. Scholtz, "The Spread Spectrum Concept," IEEE Transactions on Communications, August 1977, pp. 748-755.

2. I.S. Reed, R.A. Scholtz, T.K. Truong and L.R. Welch, "The Fast Decoding of Reed-Solomon Codes Using Continued Fractions," IEEE Trans. on Inform. Theory, January 1978.

3. R.A. Scholtz and L.R. Welch, "Group Characters: Sequences with Good Correlation Properties", IEEE Trans. on Inform. Theory, September 1978.

4. N. Bekir, R.A. Scholtz and L.R. Welch, "Partial Correlation Computations for PN Sequences," Proceedings of the 1978 National Telecommunications Conference, December 1978.

5. L.R. Welch,"Spectral Shaping Without Subcarriers", 1978 International Telemetering Conference Proceedings pp. 893-896.

6. L.R. Welch and R.A. Scholtz, "Continued Fractions and Berlekamp's Algorithm, " IEEE Trans. on Information Theory, January 1979.

Papers Submitted:

1. J.D. Olsen, R.A. Scholtz and L.R. Welch, "Bent Function Sequences", submitted to IEEE Transactions on Information Theory.

Presentations:

1. "Continued Fractions and Berlekamp's Algorithm," International Symposium on Information Theory (abstract published), October 1977, presented by R.A. Scholtz.

2. "Modified Viterbi Decoder for Burst Channels," International Symposium on Information Theory (abstract published) October 1977, presented by R.A. Scholtz.

3. "Partial Correlation Computations for PN Sequences", National Telecommunications Conference, December 1978, presented by R.A. Scholtz.

4. "Spectral Shaping Without Subcarriers", International Telemetering Conference, 1978, presented by L.R. Welch.

5. "Bent Function Sequence Sets", International Symposium on Information Theory (abstract published), June 1979, presented by J.D. Olsen.